Amendments to the Drawings

The drawings have been objected to for failing to comply with 37 CFR 1.84(p)(5) because they include reference characters not mentioned in the description. This pertains to **Figure 1**, reference characters 100 and 110, and **Figure 3**, reference characters 312, 314, and 318.

In regard to reference characters 100 and 110, Applicant amended paragraph [0005] to include reference characters 100 and 110. Likewise, Applicant amended paragraphs [0043] and [0046] to include reference numbers 312, 314, and 318.

The drawings have been objected to for failing to comply with 37 CFR 1.84 (p)(4) because reference character "303" has been used to designate both "RAM" on page 14, "operating system" on page 15, line 1, and "co-processor" on page 15, paragraph 45, line 2.

Applicant amended paragraph [0043] such that reference character 318 now refers to the operating system. Furthermore, Applicant amended paragraph [0045] such that co-processor is referenced by reference character 309. Finally, Applicant amended Figure 3 to change character reference 303 for the co-processor to reference character 309. The attached replacement sheet for Figure 3 replaces the original sheet that included Figure 3.

REMARKS

Applicant respectfully requests reconsideration of the objected and rejected claims. Claims 1-24 remain in the application. Applicant amended claims 11, 12, and 23. Applicant neither added nor canceled any claims.

Objections to the Claims

Claim 12 has been objected to because of the following informality: "the method of claim 12 further comprising" deserves to state dependence to another claim other than itself.

Applicants amended claim 12 to read: the method of claim 11 further comprising, sending output from the selection function module to a permutation function module.

Claim Rejections under 35 U.S.C. § 112

Claim 21 is rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

Applicant draws Examiner's attention to C.F.R. § 1.75 (e)(2) that suggest using the phrase "wherein the improvement comprises." Because this phrase is suggested by the C.F.R. as the language to use in the claim preamble the meaning is clear. As such, Applicant respectfully submits "the improvement comprising" in claim 21 is definite because it is similar to the recommended language in C.F.R. § 1.75.

Claim Rejections Under 35 U.S.C. §103(a)

Claims 1 – 24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes et al. "NPL Handbook of Applied Cryptography" ("Menezes") and further in view of U.S. Patent Application Publication No. 2002/001562 to Lim ("Lim").

Claim 11

Applicant respectfully disagrees with the rejection because the combination of Menezes and Lim does not describe or suggest each and every element of the invention as claimed in claim 11. Applicant requests reconsideration of the rejected claim.

Claim 11 requires a method including "exclusive-oring, using an exclusive-or gate, the output from a merged permutation and expansion function module (MPE), and a sub key block" and "sending the output from the exclusive-or gate to a selection function module."

Menezes is basically an example of the prior art data standard encryption (DES) algorithm as illustrated in **Figure 1** of Applicant's application and explained in paragraphs [0005]-[0012]. Menezes discloses dividing a 64-bit plaintext into L_0 and R_0. Both L_0 and R_0 consisting of 32-bits. The encryption of this 64-bit plaintext occurs after 16 rounds. Each round involves taking the 32-bit inputs L_{i-1} and R_{i-1} from the previous round and producing the 32-bit outputs L_i and R_i. L_i is produced by setting the value equal to R_{i-1}. R_i is calculated by first expanding R_{i-1} from 32 bits to 48 bits. Next this expanded R_{i-1} is XORed with 48 bits of a key K_i. This resulting

48 bits is then put through a substitution function that results in a 32 bit output. The result from this substitution function is permutated. Finally, this permutated result is XORed with L_{i-1} to give the value for R_i.

Therefore, each round includes two XOR functions to compute R_i. Under the Menezes implementation of the full 16 rounds required to perform a full encryption or decryption of data under the data encryption standard, 32 XOR functions are in the critical path of the encryption/decryption. This implementation results in a less efficient method for encrypting or decrypting data because of the 32 XOR functions in the critical path.

Lim describes a key scheduler for an encryption apparatus using data encryption standard algorithm. Specifically, Lim describes a key scheduler including a first permutation choice unit for permuting a 56-bit block, a first register for storing left 28 bits among the 56-bit block from the first permutation choice unit in accordance with a clock signal, a second register for storing right 28 bits among the 56-bit block from the first permutation choice unit in accordance with a clock signal, a first and a second shift units for shifting the 28-bit blocks stored in the first and second registers to the left by a first predetermined number of bits and outputting shifted 28-bit blocks to the first and the second registers respectively, a second permutation choice unit, a third and a fourth shift units each for shifting the 28 bits stored in the first and the second registers to the left by a second predetermined number of bits, and a third permutation choice unit. (Lim, Summary of the Invention). The second permutation choice unit uses the 28 bits stored in the first and the second registers to generate a first subkey. (Lim, Summary of the

Invention). The third permutation choice unit uses the 28-bits stored in the third and fourth shifters to generate a second subkey. (Lim, Summary of the Invention).

Lim further describes using this key scheduler for encryption apparatus using data encryption standard algorithm in conjunction with a DES algorithm similar to that described in Menezes and that illustrated in **Figure 1** of Applicant's application and explained in paragraphs [0005]-[0012]. Lim also describes using this key scheduler for an encryption apparatus with an unrolled version of that algorithm as described in Menezes and Applicant's application. Thus this DES algorithm employs two XOR functions per round for the calculation of R_i. Therefore, 32 XOR functions are in the critical path when implementing a full 16 rounds for decrypting or encrypting.

In addition, Lim reads in paragraph [0104] "Although the preferred embodiments of the invention," a key scheduler for encryption apparatus using data encryption standard algorithm, "have been disclosed . . . those skilled in the art will appreciate that various modifications, additions, and substitutions are possible, without departing from the scope and spirit of the invention," a key scheduler for encryption apparatus using data encryption standard algorithm, "as disclosed in the accompanying claims." Modifications, additions, and substitutions by those skilled in the art in the scope and spirit of a key scheduler for encryption apparatus using data encryption standard algorithm would fail to describe or suggest Applicant's apparatus in claim 11, because Applicant's apparatus in claim 11 is not a key scheduler.

Both Menezes and Lim fail to describe or suggest each and every element of

Applicant's claim 11. Specifically, Menezes and Lim fail to describe or suggest a "exclusive-oring . . . the output from a merged permutation and expansion function (MPE), and a sub key block" or "sending the output from the exclusive-or gate to a selection function module."

These aspects of an embodiment of Applicant's claim 11 help eliminate some XOR gates from the critical path as compared to the prior art, thus significantly improving the efficiency with which data is encrypted and/or decrypted. (Application, para. [0037]).

Because Menezes and Lim do not describe or suggest "exclusive-oring . . . the output from a merged permutation and expansion function (MPE), and a sub key block" or "sending the output from the exclusive-or gate to a selection function module," the combination of Menezes and Lim fails to render claim 11 obvious.

Claims 12 and 13

Applicant respectfully submits that claims 12 and 13 depend on independent claim 11 and include all the limitations of claim 11. As such, the combination of Menezes and Lim fails to render claims 12 and 13 obvious for at least the same reasons as claim 11.

Claim 1

Applicant respectfully disagrees with the rejection because the combination of Menezes and Lim does not describe or suggest each and every element of the invention as claimed in claim 1. Applicant requests reconsideration of the rejected claim.

Claim 1 requires an apparatus including a first merged L component key XOR gate where a left expansion module, a first merged permutation and expansion function (MPE) module, and a second selection function module (SFM) are coupled thereto. The second SFM has a first output and a second output. A second merged L component key XOR gate coupled to a right expansion module. A third merged L component key XOR gate coupled to the left expansion module, and the first MPE module. A key XOR gate coupled to a right expansion module and a first selection function module (SFM). The first SFM having outputs coupled to a first merged permutation and expansion function (MPE) module and a first permutation function module (PFM). A second collected L component XOR gate coupled to the first PFM. A first collected L component XOR gate coupled to the second PFM. The second PFM also coupled to the first output of the second SFM.

As discussed above, Menezes describes a DES algorithm where each round includes two XOR functions to compute R_i. Under the Menezes implementation of the full 16 rounds required to perform a full encryption or decryption of data under the data encryption standard, 32 XOR functions are in the critical path of the encryption/decryption. This implementation results in a less efficient method for encrypting or decrypting data because of the 32 XOR functions in the critical path.

As discussed above, Lim describes a key scheduler for an encryption apparatus using data encryption standard algorithm and a DES algorithm similar to that described in Menezes. As such, this DES algorithm employs two XOR functions per round for the calculation of R_i. Therefore, 32 XOR functions are in the critical path when implementing a full 16 rounds for decrypting or encrypting.

Moreover, modifications, additions, and substitutions by those skilled in the art in the scope and spirit of a key scheduler for encryption apparatus using data encryption standard algorithm would fail to describe or suggest Applicant's apparatus in claim 11, because Applicant's apparatus in claim 11 is not a key scheduler.

Both Menezes and Lim fail to describe or suggest each and every element of Applicant's claim 1. Specifically, Menezes and Lim fail to describe or suggest a "left expansion module coupled to a first merged L component key XOR gate and to a third merged L component key XOR gate," where the first merged L component key XOR gate is "coupled to a second SFM having a first output and a second output." Furthermore, Menezes and Lim fail to describe or suggest "a right expansion module coupled to a key XOR gate, and to a second merged L component key XOR gate." The Menezes and Lim reference further fail to describe or disclose an apparatus including an "key XOR gate coupled to a first selection function module (SFM) . . . having a first and second output," where the SFM is "coupled to a first permutation function module (PFM) and . . . a first permutation and expansion function (MPE) module."

These aspects of an embodiment of Applicant's claim 1 help eliminate some XOR gates from the critical path as compared to the prior art, thus significantly improving the efficiency with which data is encrypted and/or decrypted. (Application, para. [0037]).

Because Menezes and Lim do not describe or suggest a "left expansion module coupled to a first merged L component key XOR gate and to a third merged L component key XOR gate," where the first merged L component key XOR gate is "coupled to a second SFM having a first output and a second output;" "a right expansion module coupled to a key XOR gate, and to a second merged L component key XOR gate;" or a "key XOR gate coupled to a first selection function module (SFM) . . . having a first and second output," where the SFM is "coupled to a first permutation function module (PFM) and . . . a first permutation and expansion function (MPE) module," the combination fails to render claim 1 obvious.

Claims 2-7

Applicant respectfully submits that claims 2-7 depend on independent claim 1 and include all the limitations of claim 1. As such, the combination of Menezes and Lim fails to render claims 2-7 obvious for at least the same reasons as claim 1.

Claim 8

Applicant respectfully disagrees with the rejection because the combination of Menezes and Lim does not describe or suggest each and every element of the invention as claimed in claim 8. Applicant requests reconsideration of the rejected claim.

Claim 8 requires a method to encrypt a block of data including splitting, expanding, and exclusive-oring data. Specifically, claim 8 includes "Splitting the block of data into a left data block and a right data block." The method further requires "expanding the left data block and the right data block," "exclusive-oring, using a key gate, the right expanded data block and a first key," and "sending the output from the key XOR gate to a first selection function module (SFM)." Moreover, claim 8 requires "sending data . . . of the first SFM to a first permutation module (PFM)" and "to a first merged permutation and expansion function module (MPE)." Claim 8 also requires "exclusive-oring, using a first merged L component key XOR gate, the output from the first MPE, a second sub key and the expanded left data block" and "sending the output . . . to a second SFM." Furthermore, claim 8 includes "sending data . . . of the second SFM to a second PFM" and "to a second MPE." The method further includes "exclusive-oring, using a second merged L component key XOR gate, the output from the second MPE, a third sub key, and the expanded right data block" and "sending the output . . . to a third SFM." Moreover, the method requires "sending data from . . . the third SFM to a third PFM" and ". . . a third MPE." In addition, claim 8 requires "exclusive-oring, using a third merged L component key XOR gate, the output from the third MPE, a fourth key block, the left expanded data block, and the first MPE." Lastly, the method includes "sending the output form the second merged L component key XOR gate to a fourth SFM" and "the output from the fourth SFM to a fourth PFM."

As discussed above, Menezes describes a DES algorithm where each round includes two XOR functions to compute R_i. Under the Menezes implementation of the full 16 rounds required to perform a full encryption or decryption of data under the data encryption standard, 32 XOR functions are in the critical path of the encryption/decryption. This implementation results in a less efficient method for encrypting or decrypting data because of the 32 XOR functions in the critical path.

As discussed above, Lim describes a key scheduler for an encryption apparatus using data encryption standard algorithm and a DES algorithm similar to that described in Menezes. As such, this DES algorithm employs two XOR functions per round for the calculation of R_i. Therefore, 32 XOR functions are in the critical path when implementing a full 16 rounds for decrypting or encrypting.

Moreover, modifications, additions, and substitutions by those skilled in the art in the scope and spirit of a key scheduler for encryption apparatus using data encryption standard algorithm would fail to describe or suggest Applicant's apparatus in claim 8, because Applicant's method in claim 8 is not a key scheduler.

Both Menezes and Lim fail to describe or suggest each and every element of Applicant's claim 8. Specifically, Menezes and Lim fail to describe or suggest a method including "expanding the left data block." Moreover, there is no description or suggestion of a "first selection function module (SFM), having a first output . . . sending data . . . to a first permutation module (PFM)" and "a second output . . . sending data . . . to a first merged permutation and expansion function module (MPE)." Menezes and Lim also fail to describe or suggest "exclusive-oring, using a first merged L component key XOR gate, the output from the first MPE, a second sub key and the expended left data block," and "sending the output from the first merged L component key XOR gate to a second SFM." Likewise, Menezes and Lim fail to describe or suggest this second SFM "sending data . . . to a second PFM" and "to a second MPE." Furthermore, Menezes and Lim fail to describe or suggest "exclusive-oring, using a second merged L component key XOR gate, the output from the second MPE, third sub key, and the expanded right data block" where this merged L component key XOR gate sends its output to a third SFM. Another aspect not described or suggested includes "sending data from the . . . output of the third SFM to a third PFM" and ". . . to a third MPE." Menezes and Lim also fail to describe "exclusive-oring, using a third merged L component key XOR gate, the output from the third MPE, a fourth key block, the left expanded data block, and the first MPE."

These aspects of an embodiment of Applicant's claim 8 help eliminate some XOR gates from the critical path as compared to the prior art, thus significantly improving the efficiency with which data is encrypted and/or decrypted. (Application, para. [0037]).

Because Menezes and Lim do not describe or suggest a method including "expanding the left data block;" "sending data at the first output of" a first, second, and third SFM to a first, second, and third PFM, respectively; "sending data at the second output of the" first, second and third SFM to a first, second, and third MPE, respectively; "exclusive-oring" three inputs, using a" first and second merged L component key XOR gate, including the output from the first and second MPE, respectively, a sub key, and the expanded left and expanded right data block, respectively; or "exclusive-oring four inputs, using a third merged L component key XOR gate, including "the output from a third MPE, a fourth key block, the left expanded data block, and the first MPE; the combination of Menezes and Lim fails to render obvious claim 8.

Claims 9-10

Applicant respectfully submits that claims 9-10 depend on independent claim

8 and include all the limitations of claim 8. As such, the combination of Menezes and Lim fails to render claims 9-10 obvious for at least the same reasons as claim 8.

Claim 14

Applicant respectfully disagrees with the rejection because the combination of Menezes and Lim does not describe or suggest each and every element of the invention as claimed in claim 14. Applicant requests reconsideration of the rejected claim.

Claim 14 requires an apparatus including a co-processor coupled to a bus. The "co-processor having a left expansion module . . . coupled to a first merged L component key XOR gate and a third merged L component key XOR gate," and "a right expansion module . . . coupled to a key XOR gate and a second merged L component XOR gate." Furthermore, claim 14 requires a "key XOR gate coupled to a first selection function module (SFM)" and the SFM "coupled to a first permutation function module (PFM) . . . and . . . a first merged permutation and expansion function (MPE) module." Claim 14 also requires that the first PFM is "coupled to the second collected L component XOR gate" and the first MPE is "coupled to the first merged L component key XOR gate and to the third merged L component key XOR gate." Moreover, the claim requires that the first merged L component key XOR gate is "coupled to a second SFM" with "the SFM coupled to a second PFM." In addition, the claim requires the second PFM be "coupled to a first collected L component XOR gate."

As discussed above, Menezes describes a DES algorithm where each round includes two XOR functions to compute R_i. Under the Menezes implementation of the full 16 rounds required to perform a full encryption or decryption of data under the data encryption standard, 32 XOR functions are in the critical path of the encryption/decryption. This implementation results in a less efficient method for encrypting or decrypting data because of the 32 XOR functions in the critical path.

As discussed above, Lim describes a key scheduler for an encryption apparatus using data encryption standard algorithm and a DES algorithm similar to that described in Menezes. As such, this DES algorithm employs two XOR functions per round for the calculation of R_i. Therefore, 32 XOR functions are in the critical path when implementing a full 16 rounds for decrypting or encrypting.

Moreover, modifications, additions, and substitutions by those skilled in the art in the scope and spirit of a key scheduler for encryption apparatus using data encryption standard algorithm would fail to describe or suggest Applicant's apparatus in claim 14, because Applicant's method in claim 14 is not a key scheduler.

Both Menezes and Lim fail to describe or suggest each and every element of Applicant's claim 14. Specifically, Menezes and Lim fail to describe or suggest a co-processor coupled to a bus having a "left expansion module coupled to a first merged L component key XOR gate and to a third merged L component key XOR gate," where the first merged L component key XOR gate is "coupled to a second SFM having a first output and a second output." Furthermore, Menezes and Lim fail to describe or suggest "a right expansion module coupled to a key XOR gate, and to a second merged L component key XOR gate." The Menezes and Lim reference fail to describe or disclose an apparatus including an "key XOR gate coupled to a first selection function module (SFM) . . . having a first and second output," where the first SFM is "coupled to a first permutation function module (PFM) and . . . a first permutation and expansion function (MPE) module."

These aspects of an embodiment of Applicant's claim 14 help eliminate some XOR gates from the critical path as compared to the prior art, thus significantly improving the efficiency with which data is encrypted and/or decrypted. (Application, para. [0037]).

Because Menezes and Lim do not describe or suggest a co-processor coupled to a bus having a "left expansion module coupled to a first merged L component key XOR gate and to a third merged L component key XOR gate," where the first merged L component key XOR gate is "coupled to a second SFM having a first output and a second output;" "a right expansion module coupled to a key XOR gate, and to a second merged L component key XOR gate;" or a "key XOR gate coupled to a first selection function module (SFM) . . . having a first and second output," where the SFM is "coupled to a first permutation function module (PFM) and . . . a first permutation and expansion function (MPE) module," the combination fails to render claim 14 obvious.

Claims 15-20

Applicant respectfully submits that claims 15-20 depend on independent claim 14 and include all the limitations of claim 14. As such, the combination of Menezes and Lim fails to render claims 15-20 obvious for at least the same reasons as claim

14.

Claim 21

Applicant respectfully disagrees with the rejection because the combination of Menezes and Lim does not describe or suggest each and every element of the invention as claimed in claim 21. Applicant requests reconsideration of the rejected claim.

Claim 21 requires an improvement to an apparatus to perform a DES iteration including "a DES circuit . . . that contains no L component XOR gates." The DES circuit includes "an expansion module coupled to receive an L input." Claim 21 further requires "a merged permutation expansion module, coupled to the selection module of each iteration." Moreover, claim 21 includes "a plurality of merged L component key XOR gates coupled between a different one of the merged permutation expansion modules and the selection module of the immediately following iteration in the series" and "a plurality of permutation modules each coupled to one selection module of a different iteration." In addition, claim 21 requires "a first and second collected L component XOR gates, coupled to mutually exclusive sets of the permutation modules."

Menezes discloses a DES algorithm similar to that improved upon by claim 21. As discussed above, Menezes describes a DES algorithm where each round includes two XOR functions to compute R_i. Under the Menezes implementation of the full 16 rounds required to perform a full encryption or decryption of data under the data encryption standard, 32 XOR functions are in the critical path of the encryption/decryption. This implementation results in a less efficient method for encrypting or decrypting data because of the 32 XOR functions in the critical path.

As discussed above, Lim describes a key scheduler for an encryption apparatus using data encryption standard algorithm and a DES algorithm similar to that described in Menezes. As such, this DES algorithm employs two XOR functions per round for the calculation of R_i. Therefore, 32 XOR functions are in the critical path when implementing a full 16 rounds for decrypting or encrypting.

Moreover, modifications, additions, and substitutions by those skilled in the art in the scope and spirit of a key scheduler for encryption apparatus using data encryption standard algorithm would fail to describe or suggest Applicant's apparatus in claim 21, because Applicant's method in claim 21 is not a key scheduler.

Both Menezes and Lim fail to describe or suggest each and every element of Applicant's claim 21. Specifically, Menezes and Lim fail to describe or suggest an improvement to an apparatus to perform a DES iteration that contains no L component XOR gates. Moreover, there is no description or suggestion of "an expansion module coupled to receive an L input." Menezes and Lim also fail to describe or suggest a merged permutation expansion module. Furthermore, Menezes and Lim do not describe or suggest "a plurality of merged L component key XOR gates coupled between . . . merged permutation expansion modules and . . . [a] selection module." Likewise, Menezes and Lim fail to describe or suggest "a first and second collected L component XOR gates coupled to . . . permutation modules."

These aspects of an embodiment of Applicant's claim 21 help eliminate some XOR gates from the critical path as compared to the prior art, thus significantly improving the efficiency with which data is encrypted and/or decrypted. (Application, para. [0037]).

Because Menezes and Lim do not describe or suggest a DES circuit that contains no L component XOR gates, "an expansion module coupled to receive an L input," a merged permutation expansion module, "a plurality of merged L component key XOR gates coupled between . . . merged permutation expansion modules and . . . [a] selection module," or "a first and second collected L component XOR gates coupled to . . . permutation modules," the combination fails to render claim 21 obvious.

Claim 22

Applicant respectfully submits that claim 22 depends on independent claim 21 and includes all the limitations of claim 21. As such, the combination of Menezes and Lim fails to render claim 22 obvious for at least the same reasons as claim 21.

Claim 23

Applicant respectfully disagrees with the rejection because the combination of Menezes and Lim does not describe or suggest each and every element of the invention as claimed in claim 23. Applicant requests reconsideration of the rejected claim.

Claim 23 requires an apparatus including a DES circuit having a L and R component input and including a critical path and a non-critical path. The critical path includes a first and second expansion modules, a plurality of selection function modules, a key XOR gate, a first of a plurality of permutation modules. The "first and second expansion modules respectively coupled to receive the L and R components." The plurality of selection function modules are "coupled to each other in series by a merged permutation and expansion module" that is "coupled to a merged L component key XOR gate." The first of the plurality of permutation modules is "coupled to the last of the plurality of selection function modules." The non-critical path of claim 23 includes a first and second L component collection XOR module. The first and second L component collection modules are "coupled to mutually exclusive groups of the plurality of permutation modules."

As discussed above, Menezes describes a DES algorithm where each round includes two XOR functions to compute R_i. Under the Menezes implementation of the full 16 rounds required to perform a full encryption or decryption of data under the data encryption standard, 32 XOR functions are in the critical path of the encryption/decryption. This implementation results in a less efficient method for encrypting or decrypting data because of the 32 XOR functions in the critical path.

As discussed above, Lim describes a key scheduler for an encryption apparatus using data encryption standard algorithm and a DES algorithm similar to that described in Menezes. As such, this DES algorithm employs two XOR functions per round for the calculation of R_i. Therefore, 32 XOR functions are in the critical path when implementing a full 16 rounds for decrypting or encrypting.

Moreover, modifications, additions, and substitutions by those skilled in the art in the scope and spirit of a key scheduler for encryption apparatus using data encryption standard algorithm would fail to describe or suggest Applicant's apparatus in claim 23, because Applicant's method in claim 23 is not a key scheduler.

Both Menezes and Lim fail to describe or suggest each and every element of Applicant's claim 23. Specifically, Menezes and Lim fail to describe or suggest a DES circuit including a critical path including a first expansion module coupled to receive the L component. Furthermore, Menezes and Lim fail to describe or suggest "a plurality of selection function modules coupled to each other in series by a merged permutation and expansion module coupled to a merged L component key XOR gate." Moreover, Menezes and Lim fail to describe or suggest a non-critical path including "a first and second L component XOR module . . . coupled to mutually exclusive groups of the plurality of permutation modules."

These aspects of an embodiment of Applicant's claim 23 help eliminate some XOR gates from the critical path as compared to the prior art, thus significantly improving the efficiency with which data is encrypted and/or decrypted. (Application, para. [0037]).

Because Menezes and Lim do not describe or suggest a first expansion module coupled to receive the L component, a plurality of selection function modules coupled to each other in series by a merged permutation and expansion module coupled to a merged L component key XOR gate, or a first and second L component XOR module coupled to mutually exclusive groups of the plurality of permutation modules, the combination fails to render claim 23 obvious.

Claim 24

Applicant respectfully submits that claim 24 depends on independent claim 23 and includes all the limitations of claim 23. As such, the combination of Menezes and Lim fails to render claim 24 obvious for at least the same reasons as claim 23.

Conclusion

Applicant respectfully submits that the rejections and the objection have been overcome by the remarks. Accordingly, Applicant respectfully requests the rejections and the objection be withdrawn and the claims allowed. If the allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact the undersigned at (408) 720-8300. If there are any additional charges, please charge our Deposit Account No. 02–2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 11/14, 2005

Daniel M. De Vos
Registration No. 37,813

Customer No. 08791
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030
(408) 720-8300